REMARKS

Claims 1-21 were pending in the above-identified application when last examined and are amended as indicated above.

Claims 13-21 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter.

Independent claim 13 is amended to more clearly indicate the step of "maintaining in a computing system … a key history tree with tree nodes corresponding to nodes in said hierarchy." The process of claim 13 is thus tied to a machine, "a computing system" such as illustrated by server 40 of Applicants' Fig. 4. Accordingly, claim 13 meets the requirements of the machine-or-transformation test, which the U.S. Supreme Court recently endorsed in Bilski v. Kappos, 561 U. S. (2010) as a non-exclusive test for patentable subject matter under 35 U.S.C. § 101. Accordingly, claim 13 as amended is statutory subject matter under 35 U.S.C. § 101.

Claim 14-21 depend from claim 13 and therefore inherit the statutory subject from base claim 13.

For the above reasons, Applicants request reconsideration and withdrawal of the rejection under 35 U.S.C. § 101.

Claims 1-4 and 12-16 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Pat. App. Pub. No. 2002/0059286 (Challener) in view of U.S. Pat. No. 6,049,878 (Caronni). Applicants note that introduction to this rejection in section 4, on page 3 of the Office Action does not mention claims 8 and 20, but the rejection in section 9, on page 8 of the Office Action is also applied to claims 8 and 20. Applicants respectfully traverse the rejection of claims 1-4, 8, 12-16, and 20.

Independent claim 1 distinguishes over the combination of Challener and Caronni at least by reciting, "a manager for maintaining, on the basis of the received records, a key history tree with tree nodes corresponding to nodes in said hierarchy, the manager being arranged to store in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded." The combination of Challener and Caronni fails to suggest a manager using received records to maintain a key history tree as recited in claim 1.

PATENT LAW OFFICE OF DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

Challener is directed to trusted computing platforms, which in order to comply with Trusted Computing Platform Alliance (TCPA) standard must use 2048-bit RSA strings in a tree structure. Challener is particularly concerned with the 2048 bit lengths of the strings required by the TCPA standard because the long keys make some manipulations slow. See paragraphs [0003] and [0004] of Challener. Challener teaches that use of a second tree structure that matches TCPA tree but contains keys of other types that require less time to manipulate, can improve performance of a trusted computing platform. Neither of the tree structures disclosed by Challener are related to key updates or consolidation of key updates used for secure group communications.

Caronni is directed to multicasting of data to group members or participants and discloses use of a hierarchy of encryption keys, where each key has version information, i.e., a version number and a revision number. The version information Caronni discloses can be used when sending key updates to participants. See Caronni, column 6, lines 37-39. With Caronni's system, each participant maintains only the keys in a branch of the hierarchy specifically associated with the participant. As described by Caronni, participants can update their keys using the revision number and a one-way hash function when a participant is added to the group, but participants require new keys from the group key manager when a participant is deleted from the group. The key management process of Caronni addresses the problem of missed update messages by having the group key manager send periodic "heartbeat" messages to participants, so that any participant that has missed a key update can resynchronize with the group. See Caronni, column 7, lines 7-22. Caronni does not suggest a manager that constructs a key history tree based on records such as update messages.

In regard to a manager as recited in claim 1, the Office Action cites Challener and particularly Fig. 1 and paragraph [0021] of Challener. Challener in paragraph [0021] describes a trusted platform module (TPM), which contains protected storage for encryption keys. Challener further discloses that the encryption keys may themselves be encrypted using other keys and teaches that migratable keys may be migrated to a new platform. However, Challener does not suggest "a manager for maintaining, on the basis of the received records, a key history tree." In particular, Challener fails to disclose or suggest receiving "key updates generated for members of a group, wherein the key updates are provided in records" because Challener does not disclose or suggest key updates that are associated with secure group communications. Accordingly, Challener clearly fails to disclose or suggest "a manager for

PATENT LAW OFFICE OF DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

maintaining, on the basis of the received records, a key history tree" because Challener does not indicate that the TPM ever receives or is in any way related to records for key updates.

Caronni does describe a system using key updates but fails to suggest consolidation of such updates or maintaining a key history tree based on key updates. Further, the combination of Challener and Caronni fails to indicate how the key updates of Caronni might be related to the TPM or other structures and processes that Challener describes.

In accordance with an aspect of Applicants' invention, a group member that may have missed one or more update records can use information from an apparatus of the type recited in claim 1 to construct up-to-date keys for secure communications within the group. The version information as described in Applicants' specification allows the group member to determine which keys in the group member's possession are up to date, and maintaining the key history tree allows the apparatus to efficiently consolidate and provide information that is likely to allow the group member to update their keys without re-registering or re-synchronizing with a key hierarchy manager. Challener is not directed to group communications, and Caronni does not suggest consolidating updates or maintaining a key history tree.

For the above reasons, claim 1 is patentable over Challener and Caronni.

Claims 2-4, 8, and 12 depend from claim 1 and are patentable over Challener and Caronni for at least the same reasons that claim 1 is patentable over Challener and Caronni.

Independent claim 13 distinguishes over the combination of Challener and Caronni at least by reciting, "maintaining ... on the basis of said records, a key history tree ... this tree-maintenance step comprising ... storing in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded.." As noted above, the combination of Challener and Caronni fails to disclose or suggest maintaining a key history tree because Challener is not directed to key updates in secure group communication systems and Caronni uses "heartbeat" messages, not consolidating updates. Accordingly, claim 13 is patentable over Challener and Caronni.

Claims 14-16 and 20 depend from claim 13 and are patentable over Challener and Caronni for at least the same reasons that claim 13 is patentable over Challener and Caronni.

For the above reasons, Applicants request reconsideration and withdrawal of this rejection under 35 U.S.C. § 103.

PATENT LAW OFFICE OF DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

Claims 5-7, 9-11, 17-19 and were rejected under 35 U.S.C. § 103(a) as unpatentable over Challener in view of Caronni and further in view of U.S. Pat. App. Pub. No. US 2003/0126464 (McDaniel). Applicants respectfully traverse the rejection.

Claims 5-7 and 9-11 depend from claim 1 and are patentable over the combination of Challener and Caronni for the reasons given above to show claim 1 is patentable. In particular, the combination of Challener and Caronni do not suggest maintaining a key history tree storing version information and encrypted keys associated with nodes of a key hierarchy. McDaniel is directed to enforcing security policies and describes re-keying as one process that a security policy may require. However, McDaniel like Challener is not directed to and does not describe updating members of a group that have missed update records. Accordingly, the above reasoning showing claim 1 is patentable over Challener and Caronni also applies to the combination of Challener, Caronni, and McDaniel, and claim 1 and claims 5-7 and 9-11, which depend from claim 1, are patentable over the combination of Challener, Caronni, and McDaniel.

Claims 17-19 and 21 depend from claim 13 and are similarly patentable over the combination of Challener, Caronni, and McDaniel at least because claim 13 recites, maintaining … on the basis of said records, a key history tree " and "storing in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded.." Accordingly, claim 13 and claims 17-19 and 21, which depend from claim 13, are patentable over Challener, Caronni, and McDaniel.

For the above reasons, Applicants request reconsideration and withdrawal of the rejection under 35 U.S.C. § 102.

In summary, claims 1-21 were pending in the application. This response amends claims 1, 5, 8-13, 17, 20, and 21. For the above reasons, Applicants respectfully request allowance of the application including claims 1-21 as presented above.

Respectfully submitted,

/David Millers 37396/

David Millers
Reg. No. 37,396

PATENT LAW OFFICE OF DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543